

## CLAIMS

What is claimed is:

1    1.     A method for managing access to data in a database subject to a plurality of label-based security policies, the method comprising the steps of:

3                 receiving, within a database management system, a request for performing an operation set of one or more operations on data in a table of the database;

4                 determining which policies, of the plurality of label-based policies, apply to the table based on a policy set of one or more policies associated with the table; and

5                 for each operation in the operation set, determining whether to perform the operation on a row of the table based on a set of labels associated with the row, the set

6                 of labels corresponding to the policy set.

7

1    2.     A method according to Claim 1, further comprising adding a policy column to the table for each policy in the policy set associated with the table

1    3.     A method according to Claim 2, further comprising storing a label, of the set of labels associated with the row, in a corresponding policy column of the row.

1    4.     A method according to Claim 2, said step of determining which policies apply further comprising the step of determining whether a column is a policy column.

1    5.     A method according to Claim 1, wherein the policy set associated with the table

2     includes two or more policies of the plurality of label-based policies.

- 1    6.     A method for managing access to data in a database based on a database policy set of
- 2     one or more label-based security policies, the method comprising the steps of:
- 3         registering, with a database management system, one or more package of routines,
- 4             wherein each package implements a security model that supports a model set
- 5             of one or more policies of the database policy set and each package includes
- 6             an access mediation routine;
- 7         associating a first policy of a first model set in a first package with a first table within
- 8             the database system; and
- 9         invoking the access mediation routine in the first package for determining whether to
- 10             allow operation on data in the first table based on the first policy.

  

- 1    7.     A method according to Claim 6, further comprising the step of forming each package
- 2     so that the access mediation routine conforms to a specified interface for enforcing a policy in
- 3     the database management system.

  

- 1    8.     A method according to Claim 7, said step of forming the package further comprising
- 2     including one or more administrative routines for defining a policy for the model set.

  

- 1    9.     A method according to Claim 8, said step of including one or more administrative
- 2     routines for defining a policy further comprising including one or more administrative
- 3     routines for defining a name for a particular policy; labels for the particular policy;
- 4     descriptions for the labels; and properties for the labels.

  

- 1    10.    A method according to Claim 6, further comprising the step of invoking an
- 2     administrative routine of the first package for defining the first policy.

- 1    11. A method according to Claim 10, said step invoking the administrative routine of the
- 2    first package further comprising providing to the administrative routine of the first package a
- 3    plurality of parameters including a policy name for the first policy and a plurality of label
- 4    names for labels of the first policy.
  
- 1    12. A method according to Claim 6, further comprising, in response to attempts to operate
- 2    on data in a row in the table, the step of determining that the first policy applies to the table.
  
- 1    13. A method according to Claim 6, further comprising the steps of:
  - 2       associating a second policy of a second model set in a second package with a second
  - 3       table within the database system; and
  - 4       invoking the access mediation routine in the second package for determining whether
  - 5       to allow operation on data in the second table based on the second policy.
  
- 1    14. A method according to Claim 13, wherein the second model in the second package is
- 2    the same as the first model in the first package.
  
- 1    15. A method according to Claim 13, wherein the second model in the second package is
- 2    different from the first model in the first package.
  
- 1    16. A method according to Claim 13, wherein the second table is the same as the first
- 2    table.
  
- 1    17. A method according to Claim 13, wherein the second table is different from the first
- 2    table.

1       18. A method according to Claim 6, said step of invoking the access mediation routine in  
2       the first package further comprising providing data indicating the first policy to the access  
3       mediation routine.

1       19. A method according to Claim 6, wherein.  
2                  the method further comprises the step of determining a set of allowed labels for the  
3                  first policy for a user of the database management system;  
4                  said step of invoking the access mediation routine is performed during said step of  
5                  determining the set of allowed labels; and  
6                  the user is allowed to operate on the data according to the first policy if the data is  
7                  associated with a label for the first policy and the label is included the set of  
8                  allowed labels for the first policy.

1       20. A method according to Claim 19, further comprising the step of storing the set of  
2       allowed labels in a session cache for a communication session between the database  
3       management system and the user.

1       21. A computer-readable medium carrying one or more sequences of instructions for  
2       managing access to data in a database subject to a plurality of label-based security policies,  
3       wherein execution of the one or more sequences of instructions by one or more processors  
4       causes the one or more processors to perform the steps of:  
5                  receiving a request for performing an operation set of one or more operations on data  
6                  in a table of the database;  
7                  determining which policies, of the plurality of label-based policies, apply to the table  
8                  based on a policy set of one or more policies associated with the table; and

9           for each operation in the operation set, determining whether to perform the operation  
10           on a row of the table based on a set of labels associated with the row, the set  
11           of labels corresponding to the policy set.

1     22.    A computer-readable medium according to Claim 21, wherein execution of the one or  
2    more sequences of instructions further causes the one or more processors to perform the step  
3    of adding a policy column to the table for each policy in the policy set associated with the  
4    table

1     23.    A computer-readable medium according to Claim 22, wherein execution of the one or  
2    more sequences of instructions further causes the one or more processors to perform the step  
3    of storing a label, of the set of labels associated with the row, in a corresponding policy  
4    column of the row.

1     24.    A computer-readable medium according to Claim 22, said step of determining which  
2    policies apply further comprising the step of determining whether a column is a policy  
3    column.

1     25.    A computer-readable medium according to Claim 21, wherein the policy set  
2    associated with the table includes two or more policies of the plurality of label-based policies.

- 1    26. A computer-readable medium carrying one or more sequences of instructions for
- 2    managing access to data in a database based on a database policy set of one or more label-
- 3    based security policies, wherein execution of the one or more sequences of instructions by
- 4    one or more processors causes the one or more processors to perform the steps of:
  - 5        registering, with a database management system, one or more package of routines,
  - 6            wherein each package implements a security model that supports a model set
  - 7            of one or more policies of the database policy set and each package includes
  - 8            an access mediation routine;
  - 9        associating a first policy of a first model set in a first package with a first table within
  - 10          the database system; and
  - 11        invoking the access mediation routine in the first package for determining whether to
  - 12          allow operation on data in the first table based on the first policy.
- 1    27. A computer-readable medium according to Claim 26, wherein the access mediation
- 2    routine conforms to a specified interface for enforcing a policy in the database management
- 3    system.
- 1    28. A computer-readable medium according to Claim 27, wherein the package includes
- 2    one or more administrative routines for defining a policy for the model set.
- 1    29. A computer-readable medium according to Claim 28, wherein execution of the one or
- 2    more sequences of instructions further causes the one or more processors to perform the step
- 3    of defining a name for a particular policy; labels for the particular policy; descriptions for the
- 4    labels; and properties for the labels.

1    30.    A computer-readable medium according to Claim 26, wherein execution of the one or  
2    more sequences of instructions further causes the one or more processors to perform the step  
3    of invoking an administrative routine of the first package for defining the first policy.

1    31.    A computer-readable medium according to Claim 30, said step invoking the  
2    administrative routine of the first package further comprising providing to the administrative  
3    routine of the first package a plurality of parameters including a policy name for the first  
4    policy and a plurality of label names for labels of the first policy.

1    32.    A computer-readable medium according to Claim 26, wherein execution of the one or  
2    more sequences of instructions further causes the one or more processors to perform, in  
3    response to attempts to operate on data in a row in the table, the step of determining that the  
4    first policy applies to the table.

1    33.    A computer-readable medium according to Claim 26, wherein execution of the one or  
2    more sequences of instructions further causes the one or more processors to perform the steps  
3    of:  
4         associating a second policy of a second model set in a second package with a second  
5         table within the database system; and  
6         invoking the access mediation routine in the second package for determining whether  
7         to allow operation on data in the second table based on the second policy.

1    34.    A computer-readable medium according to Claim 33, wherein the second model in  
2    the second package is the same as the first model in the first package.

1       35. A computer-readable medium according to Claim 33, wherein the second model in  
2       the second package is different from the first model in the first package.

1       36. A computer-readable medium according to Claim 33, wherein the second table is the  
2       same as the first table.

1       37. A computer-readable medium according to Claim 33, wherein the second table is  
2       different from the first table.

1       38. A computer-readable medium according to Claim 26, said step of invoking the access  
2       mediation routine in the first package further comprising providing data indicating the first  
3       policy to the access mediation routine.

1       39. A computer-readable medium according to Claim 26, wherein  
2                    execution of the one or more sequences of instructions further causes the one or more  
3                    processors to perform the step of determining a set of allowed labels for the  
4                    first policy for a user of the database management system;  
5                    said step of invoking the access mediation routine is performed during said step of  
6                    determining the set of allowed labels; and  
7                    the user is allowed to operate on the data according to the first policy if the data is  
8                    associated with a label for the first policy and the label is included the set of  
9                    allowed labels for the first policy.

1       40. A computer-readable medium according to Claim 39, wherein execution of the one or  
2 more sequences of instructions further causes the one or more processors to perform the step  
3 of storing the set of allowed labels in a session cache for a communication session between  
4 the database management system and the user.